DOCID: 4165100 ~~SECRET//COMINT//NOFORN//X1~~

SECURITY CLASSIFICATION

NSA STAFF PROCESSING FORM

TO	EXREG CONTROL NUMBER	KCC CONTROL NUMBER
DIRECTOR	92563	IG-10003-02

THRU	ACTION	EXREG SUSPENSE
D/DIR, D SECRETARIAT 6/4	☐ APPROVAL	
SUBJECT: Quarterly Report to the Intelligence Oversight Board on NSA Activities—Second Quarter FY02	☒ SIGNATURE	KCC SUSPENSE
	☐ INFORMATION	ELEMENT SUSPENSE

DISTRIBUTION

SUMMARY

PURPOSE: To forward to the Intelligence Oversight Board (IOB) of the President's Foreign Intelligence Advisory Board, via the Assistant to the Secretary of Defense for Intelligence Oversight (ATSD(IO)), NSA's quarterly report on its intelligence activities.

BACKGROUND: Executive Order 12333 and Executive Order 12863 require Intelligence Community agency heads and Intelligence Community General Counsels and Inspectors General, respectively, to report to the IOB on a quarterly basis concerning intelligence activities that they have reason to believe may be unlawful or contrary to Executive Order or Presidential Directive. The enclosed memorandum covers all reportable activities known to the Inspector General and General Counsel. Per PIOB letter of 6 August 1982, Agency heads are responsible for reporting separately any additional reportable activities known to them, unless the President has specifically instructed that the Board is not to be informed. The Director's signature signifies that no other activities that require reporting are known to him.

RECOMMENDATION: Director sign the enclosed memorandum.

Approved for Release by NSA on 12-19-2014, FOIA Case # 70809 (Litigation)

(b)(3)-P.L. 86-36

DECLASSIFY UPON REMOVAL OF THE ENCLOSURE(S)

COORDINATION/APPROVAL

OFFICE	NAME AND DATE	SECURE PHONE	OFFICE	NAME AND DATE	SECURE PHONE
GC	Robert Deitz 30 May 02	5548s			
AGC(O)	3/31	3121s			
IG	Joel F. Brenner	3544s			
D/SEC	6/3	963-3201			

	ORG.	PHONE (Secure)	DATE PREPARED
	D11	963-3544	23 May 2002

FORM A6796 FEB 94
NSN: 7540-FM-001-5465

DERIVED FROM: NSA/CSSM 123-2
DATED: 24 February 1998
DECLASSIFY ON: X1

SECURITY CLASSIFICATION

~~SECRET//COMINT//NOFORN//X1~~

DOCID: 4165180

NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE

Office of the Inspector General

COMMERCIAL NUMBER: [redacted] (STU-III)
SECURE NUMBER: 963-3544

DATE: 10 JUNE
TO: [redacted] (b)(3)-P.L. 86-36
ORG: ATSD(IO)
FAX NUMBER: 703-275-6589
PASS TO: MATT
PHONE: 703-275-6550
NUMBER OF PAGES TO FOLLOW: 10 (+cover)
RECEIPT BY:
ACCESS LEVEL CONFIRMED: (YES) NO

FROM: [redacted] (b)(3)-P.L. 86-36
COMMENTS: Advance of Quarterly.
Signed Original is in the mail.

~~S//SI//NF~~
CLASSIFICATION

~~SECRET//COMINT//NOFORN//X1~~

NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE
FORT GEORGE G. MEADE, MARYLAND 20755-6000

6 June 2002

MEMORANDUM FOR THE CHAIRMAN, INTELLIGENCE OVERSIGHT BOARD

THRU: Assistant to the Secretary of Defense (Intelligence Oversight)

SUBJECT: (U) Report to the Intelligence Oversight Board on NSA Activities - INFORMATION MEMORANDUM

(U) Except as previously reported to you or otherwise stated in the enclosure, we have no reason to believe that any intelligence activities of the National Security Agency during the quarter ending 31 March 2002 were unlawful or contrary to Executive Order or Presidential Directive, and thus required to be reported pursuant to Section 1.7.(d) of Executive Order 12333.

(U) The Inspector General and the General Counsel continue to exercise oversight of Agency activities by means of inspections, surveys, training, review of directives and guidelines, and advice and counsel. These activities and other data requested by the Board or members of the staff of the Assistant to the Secretary of Defense (Intelligence Oversight) are described in the enclosure.

JOEL F. BRENNER
Inspector General

ROBERT L. DEITZ
General Counsel

(U) I concur in the report of the Inspector General and the General Counsel and hereby make it our combined report.

MICHAEL V. HAYDEN
Lieutenant General, USAF
Director, NSA/Chief, CSS

Encl:
a/s

This Memorandum is Unclassified
Upon Removal of Enclosure

DERIVED FROM: NSA/CSSM 123-2
DATED: 24 FEB 98
DECLASSIFY ON: X1

~~SECRET//COMINT//NOFORN//X1~~

1. (U) INSPECTOR GENERAL ACTIVITIES

a. (U//~~FOUO~~) During this quarter, the Office of Inspector General (OIG) reviewed various reports of inadvertent violations of the Attorney General (AG) procedures, as well as Department of Defense (DoD) and internal directives, to determine if corrective action was appropriate.

(b)(3)-P.L. 86-36

b. (U//~~FOUO~~) The OIG completed two inspections during this quarter. The Office of [redacted] intelligence oversight (I/O) program was found to be in need of improvement. It was recommended that the organization assign a point of contact for I/O to serve as the local authority on I/O matters. Also, it was recommended that the organization publish policy and procedures that include refresher and newcomer training, reporting violations, and quarterly reporting. Management concurred in the recommendations and indicated they would be implemented by 1 June 2002. A joint inspector general team completed an inspection of the Fort Gordon Regional Security Operations Center (GRSOC). The I/O new employee and refresher training programs were found to meet DoD and NSA requirements. The inspection team noted that I/O training reminders such as posters and policy letters were sparse throughout GRSOC spaces. It was recommended that the GRSOC and Service Cryptologic Elements design and post I/O training reminders in conspicuous locations throughout the GRSOC.

c. (U//~~FOUO~~) The OIG is providing guidance and assistance to various organizations that have requested help in establishing intelligence oversight training programs. These requests resulted from recommendations in our report entitled *Strategic Assessment of Intelligence Oversight* that we issued on 14 December 2001; it was sent to all Agency directorates and associate directorates.

2. (U) GENERAL COUNSEL ACTIVITIES

a. ~~(C//SI)~~ The OGC reviewed various intelligence activities of the United States Signals Intelligence System (USSS) to determine whether they were conducted in accordance with applicable statutes, Executive Orders, Attorney General procedures, and DoD and internal directives. The OGC advised Agency elements on a number of questions, including the collection and dissemination of communications of or concerning U.S. persons; the reporting of possible violations of federal criminal law contained in SIGINT product; the testing of electronic equipment; and the applicability of the Foreign Intelligence Surveillance Act (FISA). With few exceptions, the issues presented were routine and indicated that the operating elements understand the restrictions on SIGINT operations. The OGC did not file any reports with the Intelligence Oversight Board during this quarter.

3. (U) SIGINT ACTIVITIES

a. ~~(S//SI)~~ Collection Against U.S. Persons

(1) (U) Intentional

~~(S//SI)~~ During this quarter, the DIRNSA granted approval for consensual collection against [ ] persons; DIRNSA-approved consensual collection against [ ] U.S. persons was routinely terminated this quarter. (b)(1) (b)(3)-P.L. 86-36

~~(S//SI)~~ The Attorney General granted authority to collect the communications of [ ] U.S. persons during this quarter. (b)(3)-P.L. 86-36

(2) (U) Unintentional

~~(S//SI)~~ This quarter, unintentional retrieval strategies using the [ ] raw traffic files resulted in [ ] incidents against U.S. persons. All incidents were reported to responsible oversight officials and investigated; corrective actions were taken.

b. (U//~~FOUO~~) Dissemination of U.S. Identities

(b)(1) (b)(3)-P.L. 86-36

(1) (U) Intentional

~~(S//SI)~~ In accordance with section 7 of USSID 18, [ ] U.S. identities were disseminated. The following table shows the justification and the number of instances of dissemination: in the "Unmasked" column, the U.S. identity was revealed in a serialized end product; in the "User Requested" column, a U.S. identity was released to a user at the user's request.

JUSTIFICATION	Unmasked	User Requested	TOTAL
7.2.c Necessary			
7.2.c.1 Foreign Official			
7.2.c.3 International narcotics			
7.2.c.4 Criminal activity			
7.2.c.7 U.S. Government Official			
TOTAL			

(2) (U) Unintentional

~~(S//SI)~~ During the fourth quarter of 2001 [ ] SIGINT products were canceled because they contained the identities of U.S. persons, organizations, or entities. Of those, [ ] were reissued with the reference to the U.S. person obscured.

(b)(1)
(b)(3)-P.L. 86-36

4. (U) OTHER ACTIVITIES

(U) Integrees in Analysis and Production

~~(S//SI//NF)~~ During this quarter, [ ] In all cases, these individuals were provided with USSID 18 training. Organizations having integrees at NSA included [ ]

(U) [ ]

(b)(1)
(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36

~~(S//SI)~~ [ ] provided support to [ ] during the quarter. This support included [ ] Support was also provided to [ ] who requested [ ] assistance [ ]

(b)(3)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)

(U) OGC Legal Authorities Briefing

(U//~~FOUO~~) As reported last quarter, the SID has engaged the OGC to present a series of briefings on NSA's legal authorities and restrictions to the entire SID workforce (civilians, military, contractors and integrees). The briefings are geared toward a broad understanding of the fundamental legal principles underlying the SID mission. At the briefings, each individual is given handouts containing a list of all the legal documents that must be read on a yearly basis, procedures for handling a USSID-18 violation, and points of contact for specific oversight issues in the SID Oversight and Compliance Office. The first briefing was presented on 6 September; after a 2-month hiatus related to the September 2001 terrorist attacks, briefings resumed on 6 November. The briefings have been

(b)(1)
(b)(3)-P.L. 86-36

completed; approximately [redacted] SID personnel received the briefings live, while other SID and Agency personnel viewed the presentation remotely or via videotape.

(U) Policy Guidance Issued

~~(S//SI)~~ The Signals Intelligence Director issued a policy memorandum concerning access to raw SIGINT traffic in order to ensure that the activities regarding access to raw traffic are consistent with NSA authorities under Executive Order 12333 and implementing regulations and directives. The memorandum, entitled *Signals Intelligence Policy on Raw Traffic Access and the SIGINT Production Chain*, dated 14 January 2002, provides definitions for "raw traffic" and the "SIGINT production chain" and provides clear guidance for eligibility for access to raw SIGINT information. The memorandum is enclosed as attachment A.

(U) Databases

~~(S//SI)~~ Numerous branches in [redacted] under OGC guidance, that [redacted] to avoid USSID-18 violations. Only information that is essential to understanding the intelligence is included. [redacted] Additionally, many Offices of Primary Interest [redacted] in order to ensure that they are not collected against or named in product.

(b)(1)
(b)(3)-P.L. 86-36

~~SECRET//COMINT//X1~~

UNITED STATES GOVERNMENT

memorandum

DATE: 14 January 2002

SID-001-02

REPLY TO ATTN OF: Signals Intelligence Director

SUBJECT: (U//~~FOUO~~) Signals Intelligence Policy on Raw Traffic Access and the SIGINT Production Chain - POLICY MEMORANDUM

TO: SIGINT Directorate, SIGINT/Extended Enterprise

(U) Policy

~~(C)~~ United States SIGINT System (USSS) personnel and others who participate in the SIGINT production process are authorized to share raw traffic only with those individuals in the SIGINT production chain. In order to ensure our activities are consistent with our authorities under Executive Order 12333 and implementing regulations and directives, the USSS must apply consistent definitions of "raw traffic" and the "SIGINT production chain" as put forth in this document. Eligibility for access to raw traffic will be assessed based on the requester's role in the SIGINT Production chain.

NOTE: Being part of the SIGINT production chain does not imply automatic access to all types of data or information, but rather ***eligibility*** for access with a substantiated justification. Oversight and need-to-know issues must be addressed prior to granting access.

(U//~~FOUO~~) Definition of Raw Traffic

~~(C//SI)~~ **Raw Traffic** is any signals intelligence acquired either as a result of search and development or collection operations in support of foreign intelligence requirements **BEFORE** the information has been evaluated for foreign intelligence **AND** minimization purposes.

NOTE: After data has been minimized and has been determined to constitute foreign intelligence, it can then be considered eligible for release in accordance with approved SIGINT delivery vehicles and processes established by USSS SIGINT reporting policies.

(U//~~FOUO~~) Definition of SIGINT Production Chain

~~(S//SI)~~ The term **"SIGINT production chain"** describes the group of individuals of diverse responsibilities who contribute to the production of SIGINT. There is no single SIGINT production chain at NSA, and, in fact, your immediate SIGINT production chain may vary depending on the target or project on which you are working or the SIGINT that you plan to disseminate. In general, the SIGINT production chain is composed of SIGINT production personnel--collectors, cryptanalysts, intelligence analysts, linguists, reporters, SIGINT development analysts, staff and support elements, and managers--necessary for the production of SIGINT under NSA authorities. Developers of these processes may also be considered members of the SIGINT Production Chain depending on the nature of their projects or programs. The following are examples of how the chain can change depending on circumstances:

(Example 1: ~~(S//SI)~~ [redacted] (b)(1) 86-36

[redacted]

Derived from: NSA/CSSM 123/2
Dated: 24 February 1998
Declassify on: X1

(Example 2: ~~(S//SI)~~

(Example 3: ~~(S//SI)~~

(b)(1)
(b)(3)-P.L. 86-36

~~(C)~~ Members of the SIGINT Production Chain

~~(S//SI)~~ The SIGINT production chain consists of SIGINT production personnel who are directly involved in the development, collection, processing, analysis, retention or dissemination of SIGINT, and sometimes in program or project development to support these processes. Those with direct management or oversight responsibilities over those processes are also part of the SIGINT production chain.

~~(S//SI)~~ Although the members of the SIGINT production chain may change under varying circumstances, in general, they fall into the following categories of SIGINT production personnel:

(b)(3)-P.L. 86-36

~~(S//SI)~~ Typically, the personnel cited above will be found in SIGINT production elements and SIGINT field sites and will be considered eligible for access to raw traffic. The next list depicts SIGINT production elements that are most likely to employ SIGINT production personnel. However, an

individual is not automatically eligible for access to raw traffic simply by virtue of organizational assignment; not all personnel require access. Likewise, an individual's organizational designator is not a bar to being considered part of SIGINT production if the individual meets other criteria. Each individual's need-to-know must be established, and an oversight process must be in place, prior to access being granted.

~~(C)~~ SIGINT Producers

~~(S//SI)~~ The following **elements** typically employ SIGINT production personnel and are considered to be part of the SIGINT production chain, provided that they meet the defined criteria. (This list is not exclusive; special circumstances are addressed in the final section.)

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36

~~(S//SI)~~ **Individuals** integrated into SIGINT production elements typically become SIGINT production personnel for the duration of the integration or detail. Integration occurs frequently in the following situations, though other circumstances might also result in this type of arrangement:

-
-
-
-

(b)(3)-P.L. 86-36

~~(S)~~ Third Parties

~~(S)~~

~~(S)~~

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

~~(C)~~ Non-SIGINT Producers

~~(S//SI)~~ The following elements typically employ **NO** SIGINT production personnel and are **not** considered to be part of the SIGINT production chain. Exceptions to this rule due to special circumstances must be approved by the Signals Intelligence Director, and only personnel exercising DIRNSA's SIGINT authority are eligible for exceptions. (See the final section of this document.)

(U) Special Circumstances

(b)(3)-P.L. 86-36

~~(C)~~ In order to maintain the flexibility of the SIGINT system to respond to intelligence needs, the SIGINT Director may designate a specific activity as supporting SIGINT production in cases where the usual definitions seem not to apply. The SIGINT Director may either initiate such a designation, or an element typically considered to be outside of the SIGINT production chain may request that the Signals Intelligence Director extend SIGINT production responsibilities to it based on mission requirements. The individual's or element's management chain must submit a request for consideration of its special circumstances to the Signals Intelligence Director, through SID/Oversight and Compliance (**NOTE**: if requestor is external to NSA/W, the request should first be submitted to the SID/Extended Enterprise for further coordination with SID/Oversight and Compliance.) The request should present a compelling case for an individual or element to be granted exceptional status as a member of the SIGINT production chain as a first stage in meeting eligibility requirements for raw traffic access. At a minimum the request should include:

(b)(1)
(b)(3)-P.L. 86-36

~~(S//SI)~~ SID/Oversight and Compliance will evaluate each request in consultation with the Office of General Counsel, staffing the request through other elements as appropriate. Based on the findings from this process, SID/Oversight and Compliance will formulate a recommended disposition of the request to the Signals Intelligence Director for consideration. The Signals Intelligence Director will determine whether the individual or element will be recognized as a member of the SIGINT production chain, and the duration of this recognition, thereby making the entity ***eligible*** for access to raw traffic. (Note: Within the SIGINT Directorate and for additional NSA elements, the Signals Intelligence Director has wide discretion to make this determination; however, if the element in question is outside NSA, additional documentation, e.g., a Memorandum of Understanding with an outside organization, will likely be required for implementation.) Access requests for particular raw traffic data sources will be made through SID/Oversight and Compliance on a case-by-case basis.

/s/

MAUREEN A. BAGINSKI
Signals Intelligence Director